サイバーセキュリティ保証レベル（CAL）の積極活用

今回のメルマガでは、自動車サイバーセキュリティ規格 ISO/SAE 21434 に示される「サイバーセキュリティ保証レベル（CAL）」の活用についてお話しします。CAL は機能安全における ASIL に相当し、サイバーセキュリティリスクの程度に応じて開発手法の厳密さをコントロールする仕組みです。CAL にはサイバーセキュリティ対応のコストを抑える可能性がありながら、業界内では現在のところあまり広く活用されていないようです。これはもったいない状況ですので、今回メルマガのテーマとして取り上げました。

サイバーセキュリティ関連製品の開発では、様々な追加活動が求められます。例えば、以下のような活動です。

・弱点分析、TARA
・厳密なレビュー、検証
・追加テスト（ファジング、ペネトレーションテスト）
・サイバーセキュリティアセスメント

これらは製品のセキュリティ確保に寄与しますが、開発負荷の増大も招きます。限られたリソースの中で確実かつ効率的にセキュリティを確保するには、戦略的なアプローチが必要です。

確実かつ効率的なセキュリティ確保の鍵は、「選択と集中」です。つまり、リスク分析を通じて重要な箇所を特定し、そこにリソースを重点的に投入する考え方です。この考え方は機能安全の規格 ISO 26262 においても HARA（ハザード分析及びリスクアセスメント）と ASIL という仕組みに色濃く反映されており、その仕組みは ISO/SAE 21434 にも TARA（脅威分析及びリスクアセスメント）と CAL として引き継がれています。これらの仕組みを組み合わせて活用することで、サイバーセキュリティ活動を効率的に実施できます。

とは言え、ISO/SAE 21434 における CAL の定義は Annex 扱いであり、詳細な要求は定義されていません。そのためプロセス整備の際に軽視されたり、後回しにされたりしがちです。この背景には、流動的なサイバーセキュリティ関連の情勢や、国や組織によるサイバーセキュリティリスクの捉え方の違いがあり、規格内に絶対的な基準を示しづらいという状況があったようです。しかし、CAL の活用には以下のようなメリットがあります。

・開発負荷を抑えつつ、セキュリティを高めることができる
・サイバーセキュリティ活動の選択に根拠を与え、顧客との調整や合意の土台となる

CAL を活用するにはまず組織標準として CAL の判断基準（表 1）と CAL 毎のサイバーセキュリティ活動の厳密さ（表 2）を定め、次に各製品開発プロジェクトが組織標準に従ってサイバーセキュリティ活動の選択を行います。

表 1　CAL 決定基準の例

		攻撃元区分			
		物理	ローカル	隣接	ネットワーク
影響	深刻	CAL2	CAL3	CAL4	CAL4
	重大	CAL1	CAL2	CAL3	CAL4
	中程度	CAL1	CAL1	CAL2	CAL3
	無視できる	—	—	—	—

※ISO/SAE 21434 Annex E より抜粋

表 2　CAL 毎のサイバーセキュリティ活動の厳密さの定義例　～テスト活動の実施範囲～

活動	テスト範囲			
	CAL1	CAL2	CAL3	CAL4
機能テスト	要求に対するテスト		要求およびコンポーネント間の相互作用に対するテスト	
脆弱性スキャン	既知の脆弱性に対するスキャン			
ファジング	テスト範囲に関する要求なし	ランダムデータによるファジング	より多くのランダムデータによるファジング および/または グレーボックス観点で選択したデータを含めたファジング	
ペネトレーションテスト	テスト範囲に関する要求なし		中程度の専門知識を前提としたテスト	高度な専門知識を前提としたテスト

※ISO/SAE 21434 Annex E 表 E.3 を参考に再構成

他にも CAL による活動選択はレビューの厳格さや独立性など多くの面に適用できます。CAL の効果をさらに多く引き出すには、サイバーセキュリティの観点で開発対象を領域分割し、領域毎に CAL を設定/低減する戦略が有効です。ただし、これには機能安全における ASIL の分割とは異なる原理に基づいた考え方が必要となります。サイバーセキュリティにおけるパーティショニングや CAL の低減といった詳細なテーマについては、今後無償セミナーやワークショップ等でも取り上げる予定です。ぜひ、今後の情報発信にもご注目ください。

2025/3/19 大野 貴正